Amendment to the Claims:

1. (Currently Amended) An internal security method for a relational database system, comprising the steps of:

(a) determining which data information from the total amount of data information stored in system databases is restricted data information that shall not be accessible by each and every 1 to N system users, where N is an integer greater than 1;

(b) determining for each system user the restricted data information that such a system user shall have access;

(c) creating at least one relational access table with each system user having at least one record in the relational access table and using a foreign key in the table created at step (c) that is linked to a primary key associated with a system user's table of the relational database system for controlling the system user's downstream access to the restricted data information that was determined at step (b) and preventing downstream and upstream access to unauthorized restricted data information through the use of the foreign key and primary key link; and

(d) each system user accessing restricted data information stored in the system databases according to the relational access table created at step (c).

2. (Original) The method as recited in claim 1, wherein the relational database is a structured query language database.

3. (Original) The method as recited in claim 1, wherein each relational access table has a foreign key that relates to a primary key of only one system user.

4. (Original) The method as recited in claim 1, wherein each relational access table created at step (c) may have access to additional restricted data information added to it by updating the relational access table after it is created.

5. (Original) The method as recited in claim 1, wherein each relational access table created at step (c) may have access to certain restricted data information deleted from it by updating the relational access table after it is created.

6. (Original) The method as recited in claim 1, wherein the relational database system that incorporates the internal security method includes a star schema configuration.

7. (Original) The method as recited in claim 6, wherein the relational database system that incorporates the internal security method includes a full star schema configuration.

8. (Currently Amended) A internal security method for a relational database system, comprising the steps of:

(a) determining which data information from the total amount of data information stored in system databases is restricted data information that shall not be accessible by each and every 1 to N system users, where N is an integer greater than 1;

(b) determining for each system user the restricted data information that such a system user shall have access;

(c) determining the hierarchical level of access for each system user with regard to the restricted data information;

(d) determining for at least two system users, based on the hierarchical level of access determination at step (c), that a second system user with a lower hierarchical level of access has access to the restricted data information that is a subset of the restricted data information to which a first system user with a higher hierarchical level of access has access;

(e) ~~created~~ creating at least one relational access table with each of the first and second system users having at least one record in the relational access table and using a foreign key in the table created at step (e) that is linked to a primary key associated with each of the first and second system user's table of the relational database system for controlling each of the first and second system users' respective downstream access to restricted data information that is determined at step (b) and preventing the first and second system users' respective downstream and upstream access to unauthorized restricted data information through the use of a foreign key and primary key link such that the first system user will have one or more records in the relational access table that will permit the first system user's access to restricted data information that is determined for the first system user at step (b) to be joined with the second system user's access to restricted data information that is determined for the second system user at step (b), and the second system user will have one or more records in the relational access table will

permit the second system user's access to restricted data information that is determined for the second system user at step (b); and

(f) the first and second system users accessing restricted data information stored in the system databases according to the relational access table created at step (e).

9. (Original) The method as recited in claim 8, wherein the relational database is a structured query language database.

10. (Original) The method as recited in claim 8, wherein each relational access table has a foreign key that relates to a primary key of only one system user.

11. (Original) The method as recited in claim 8, wherein each relational access table created at steps (e) and (f) may have access to additional restricted data information added to them by updating the relational access table after they are created.

12. (Original) The method as recited in claim 8, wherein each relational access table created at steps (e) and (f) may have access to certain restricted data information deleted from them by updating the relational access table after they are created.

13. (Original) The method as recited in claim 8, wherein the relational database system that incorporates the internal security method includes a star schema configuration.

14. (Original) The method as recited in claim 13, wherein the relational database system that incorporates the internal security method includes a full star schema configuration.

15. (Currently Amended) A internal security method for a relational database system, comprising the steps of:

(a) determining which data information from the total amount of data information stored in system databases is restricted data information that shall not be accessible by each and every 1 to N system users, where N is an integer greater than 1;

(b) determining for each system user the restricted data information that such a system user shall have access;

(c) determining the hierarchical level of access for each system user with regard to the restricted data information;

(d) determining for at least two system users, based on the hierarchical level of access determination at step (c), that a second system user with a lower hierarchical

level of access has access to the restricted data information that includes other than a subset of the restricted data information to which a first system user with a higher hierarchical level of access has access;

(e) ~~created~~ creating at least one relational access table with each of the first and second system users having at least one record in the relational access table and using a foreign key in the table created at step (e) that is linked to a primary key associated with each of the first and second system user's table of the relational database system for controlling each of the first and second system users' respective downstream access to restricted data information that is determined at step (b) and preventing respective downstream and upstream access to unauthorized restricted data information through the use of a foreign key and primary key link such that the first system user will have one or more records in the relational access table that will permit the first system user's access to restricted data information that is determined for the first system user at step (b) to be joined with the second system user's access to restricted data information that is determined for the second system user at step (b), and the second system user will have one or more records in the relational access table will permit the second system user's access to restricted data information that is determined for the second system user at step (b); and

(f) the first and second system users accessing restricted data information stored in the system databases according to the relational access table created at steps (e).

16. (Original) The method as recited in claim 15, wherein the relational database is a structured query language database.

17. (Original) The method as recited in claim 15, wherein each relational access table has a foreign key that relates to a primary key of only one system user.

18. (Original) The method as recited in claim 15, wherein each relational access table created at steps (e) and (f) may have access to additional restricted data information added them by updating the relational access table after they are created.

19. (Original) The method as recited in claim 15, wherein each relational access table crated at steps (e) and (f) may have access to certain restricted data information deleted from them by updating the relational access table after they are created.

20. (Original) The method as recited in claim 15, wherein the relational database system that incorporates the internal security method includes a star schema configuration.

21. (Original) The method as recited in claim 20, wherein the relational database system that incorporates the internal security method includes a full star schema configuration.

22. (Currently Amended) A internal security method for a relational database system, comprising the steps of:

(a) determining which data information from the total amount of data information stored in system databases is restricted data information that shall not be accessible by each and every 1 to N system users, where N is an integer greater than 1;

(b) determining for each system user the restricted data information that such a system user shall have access;

(c) determining the hierarchical level of access for each system user with regard to the restricted data information;

(d) determining for at least two system users, based on the hierarchical level of access determination at step (c), that a second system user with a lower hierarchical level of access has access to the restricted data information that is a subset and includes other than a subset of the restricted data information to which a first system user with a higher hierarchical level of access has access;

(e) ~~created~~ creating at least one relational access table with each of the first and second system users having at least one record in the relational access table and using a foreign key in the table created at step (e) that is linked to a primary key associated with each of the first and second system user's table of the relational database system for controlling each of the first and second system users ' respective downstream access to restricted data information that is determined at step (b) and preventing respective downstream and upstream access to unauthorized restricted data information through the use of a foreign key and primary key link such that the first system user will have one or more records in the relational access table that will permit the first system user's access to restricted data information that is determined for the first system user at step (b) to be joined with the second system user's access to restricted data information

that is determined for the second system user at step (b), and the second system user will have one or more records in the relational access table will permit the second system user's access to restricted data information that is determined for the second system user at step (b); and

(f) the first and second system users accessing restricted data information stored in the system databases according to the relational access table created at steps (e).

23. (Original) The method as recited in claim 22, wherein the relational database is a structured query language database.

24. (Original) The method as recited in claim 22, wherein each relational access table has a foreign key that relates to a primary key of only one system user.

25. (Original) The method as recited in claim 22, wherein each relational access table created at steps (e) and (f) may have access to additional restricted data information added to them by updating the relational access table after they are created.

26. (Original) The method as recited in claim 22, wherein each relational access table created at steps (e) and (f) may have access to certain restricted data information deleted from them by updating the relational access table after they are created.

27. (Original) The method as recited in claim 22, wherein the relational database system that incorporates the internal security method includes a star schema configuration.

28. (Original) The method as recited in claim 27, wherein the relational database system that incorporates the internal security method includes a full star schema configuration.